

WHAT IS CLAIMED IS:

- 1 1. A method of generating an output symbol, wherein the output symbol is selected
2 from an output alphabet and the output symbol is such that an input file, comprising an
3 ordered plurality of input symbols each selected from an input alphabet, is recoverable
4 from a set of such output symbols, the method comprising the steps of:
5 obtaining a key I for the output symbol, wherein the key is selected from a key
6 alphabet and the number of possible keys in the key alphabet is much larger than
7 the number of input symbols in the input file;
8 calculating, according to a predetermined function of I , a list $AL(I)$ for the output
9 symbol, wherein $AL(I)$ is an indication of $W(I)$ associated input symbols
10 associated with the output symbol, and wherein weights W are positive integers
11 that vary between at least two values and are greater than one for at least one
12 value of I ; and
13 generating an output symbol value $B(I)$ from a predetermined function of the
14 associated input symbols indicated by $AL(I)$.
- 1 2. The method of claim 1, wherein the step of obtaining key I comprises a step of
2 calculating key I according to a random function or pseudorandom function.
- 1 3. The method of claim 1, wherein the step of calculating comprises a step of
2 calculating $W(I)$ according to a random function or pseudorandom function of I .
- 1 4. The method of claim 1, wherein the step of calculating comprises a step of
2 calculating $AL(I)$ according to a random function or pseudorandom function of I .
- 1 5. The method of claim 1, wherein the step of calculating comprises the steps of:
2 calculating, according to a predetermined function of I and a probability distribution,
3 a weight $W(I)$, wherein the probability distribution is over at least two positive
4 integers, at least one of which is greater than one;
5 calculating a list entry for list $AL(I)$; and
6 repeating the step of calculating a list entry for list $AL(I)$ until $W(I)$ list entries are
7 calculated.

1 6. The method of claim 5, wherein the step of calculating $W(I)$ comprises a step of
 2 determining $W(I)$ such that W approximates a predetermined distribution over the key
 3 alphabet.

1 7. The method of claim 6, wherein the predetermined distribution is a uniform
 2 distribution.

1 8. The method of claim 6, wherein the predetermined distribution is a bell curve
 2 distribution.

1 9. The method of claim 6, wherein the predetermined distribution is such that $W=1$
 2 has a probability of $1/K$, where K is the number of input symbols in the input file, and
 3 $W=i$ has a probability of $1/i(i-1)$ for $i=2, \dots, K$.

1 10. The method of claim 1, wherein the predetermined function of the associated
 2 input symbols indicated by $AL(I)$ is an exclusive OR (XOR) of the input symbols
 3 indicated by $AL(I)$.

1 11. The method of claim 1, wherein the input alphabet and the output alphabet are
 2 the same alphabet.

1 12. The method of claim 1, wherein the input alphabet comprises 2^{M_i} symbols and
 2 each input symbol encodes M_i bits and wherein the output alphabet comprises 2^{M_o}
 3 symbols and each output symbol encodes M_o bits.

1 13. The method of claim 1, wherein each subsequent key I is one greater than the
 2 preceding key.

1 14. A method of encoding a plurality of output symbols, each according to claim 1,
 2 the method further comprising steps of:
 3 generating key I for each of the output symbols to be generated; and
 4 outputting each of the generated output symbols as an output sequence to be
 5 transmitted through a data erasure channel.

1 15. The method of claim 14, wherein each key I is selected independently of other
 2 selected keys.

1 16. A method of transmitting data from a source to a destination over a packet
2 communication channel, comprising the steps of:

- 3 a) arranging the data to be transmitted as an ordered set of input symbols, each
4 selected from an input alphabet and having a position in the data;
- 5 b) generating a plurality of output symbols, each selected from an output alphabet,
6 wherein each output symbol of the plurality of output symbols is generated by the
7 steps of:
 - 8 1) selecting, from a key alphabet, a key I for the output symbol being generated;
 - 9 2) determining a weight, $W(I)$, as a function of I , wherein weights W are positive
10 integers that vary between at least two values and over the key alphabet and
11 are greater than one for at least some keys in the key alphabet;
 - 12 3) selecting $W(I)$ of the input symbols according to a function of I , thus forming
13 a list $AL(I)$ of $W(I)$ input symbols associated with the output symbol; and
 - 14 4) calculating a value $B(I)$ of the output symbol from a predetermined value
15 function of the associated $W(I)$ input symbols;
- 16 c) packetizing at least one of the plurality of output symbols into each of a plurality
17 of packets;
- 18 d) transmitting the plurality of packets over the packet communication channel;
- 19 e) receiving at least some of the plurality of packets at the destination; and
- 20 f) decoding the data from the plurality of received packets.

1 17. The method of claim 16, wherein the step of decoding the data comprises the
2 steps of:

- 3 1) processing each received output symbol by the steps of:
 - 4 a) determining the key I for the output symbol;
 - 5 b) determining the weight $W(I)$ for the output symbol; and
 - 6 c) determining the $W(I)$ associated input symbols for the output symbol;
- 7 2) determining if enough information is received to decode any input symbols; and
- 8 3) decoding input symbols that can be decoded from the information received.

1 18. The method of claim 17, wherein the step of determining the key I comprises a
2 step of at least partially determining the key I from data supplied in packets received over
3 the packet communication channel.

1 19. The method of claim 16, wherein the step of decoding the data comprises the
2 step of:

3 1) processing each received output symbol by the steps of:

4 a) determining the weight $W(I)$ for the output symbol;

5 b) determining the $W(I)$ associated input symbols for the output symbol; and

6 c) storing the value $B(I)$ of the output symbol in an output symbol table along
7 with the weight $W(I)$ and the positions of the $W(I)$ associates for the output
8 symbol;

9 2) receiving additional output symbols and processing them according to step 1) and
10 its substeps;

11 3) for each output symbol, OS1, having a weight of one and not being denoted as a
12 used up output symbol, performing the steps of:

13 a) calculating an input symbol for an input symbol position corresponding to
14 OS1;

15 b) identifying connected output symbols in the output symbol table, wherein a
16 connected output symbol is an output symbol that is a function of the input
17 symbol processed in step 3)a);

18 c) recalculating the connected output symbols to be independent of the input
19 symbol processed in step 3)a);

20 d) decrementing by one the weights of the output symbols recalculated in step
21 3)c); and

22 e) denoting OS1 as a used up output symbol; and

23 4) repeating steps 1) through 3) above until the ordered set of input symbols is
24 recovered at the destination.

1 20. The method of claim 19, wherein the step of denoting is a step of assigning a
2 weight of zero to the used up output symbol.

1 21. The method of claim 19, wherein the step of denoting comprises a step of
2 removing the used up output symbol from the output symbol table.

1 22. The method of claim 16, wherein the step of packetizing is a step of packetizing
2 a plurality of output symbols into each packet, the method further comprising a step of

3 using an output symbol's position within a packet as a part of the key for the output
4 symbol.

1 23. The method of claim 17, wherein the step of decoding comprises the steps of:
2 sorting received output symbols by weight; and
3 processing output symbols by weight, with lower weight symbols being processed
4 before higher weight symbols.

1 24. The method of claim 1, wherein the step of calculating AL(I) comprises the steps
2 of:
3 identifying the number K of input symbols in the input file, at least approximately
4 and a weight W(I);
5 determining the smallest prime number P greater than or equal to K;
6 if P is greater than K, at least logically padding the input file with P-K padding input
7 symbols;
8 generating a first integer X such that $1 \leq X < P$ and a second integer Y such that
9 $0 \leq Y < P$;
10 setting the J-th entry in AL(I) to $((Y + (J-1) \cdot X) \bmod P)$ for each J from 1 to W(I).

1 25. The method of claim 24, wherein the step of setting the J-th entry in AL(I) for
2 each J comprises the steps of:
3 setting the first entry V[J=0] in an array V to Y;
4 setting the J-th entry V[J] in the array V to $(V[J-1] + X) \bmod P$ for each J from 1 to
5 W(I) minus one; and
6 using the array V as the list AL(I).

1 26. The method of claim 6, wherein the predetermined distribution is such that,
2 given tunable parameters R1 and R2 and K being the number of input symbols in the
3 input file, weight W=1 has a probability proportional to R1/K, weights in a low-weight
4 class ranging from weight W=2 to weight W=K/R2 - 1 have a probability proportional to
5 $1/(W(W-1)(1-W \cdot R2/K))$ and weights in a high-weight class ranging from weight
6 W=K/R2 to weight W=K have a selected probability distribution.